SOC ESSENTIALS

What I Learned Building the SOC @ St. Jude Medical

- Russ Staiger, Lead Analyst - Cyber Threat Intel - CTAC

CTAC Vision & Mission

Vision

A safe, secure and resilient information technology operating environment that provides for the protection of our patient, customer, and employee information and allows for the execution of the St. Jude Medical mission and strategy.

Mission

The Cyber Threat Action Center’s (CTAC) mission is to identify, protect against, respond to, and enhance resiliency against cyber security threats. The CTAC provides cyber security capabilities that foster excellence in the execution of St. Jude IT and business operations.

Advanced Threats Are Hard to Find

The SOC is a ‘must-have’ for enterprise and intellectual property protections.

Cyber Criminals

“Another Day, Another Retailer in a Massive Credit Card Breach”

– Bloomberg Businessweek, March 2014

Nation States/Hacktivists

“Banks Seek U.S. Help on Iran Cyber attacks”

– Wall Street Journal, Jan 2013

Insider Threats

“Edward Snowden Tells SXSW He'd Leak Those Secrets Again”

– NPR, March 2014

100%

Valid credentials were used

40

Average # of systems accessed

229

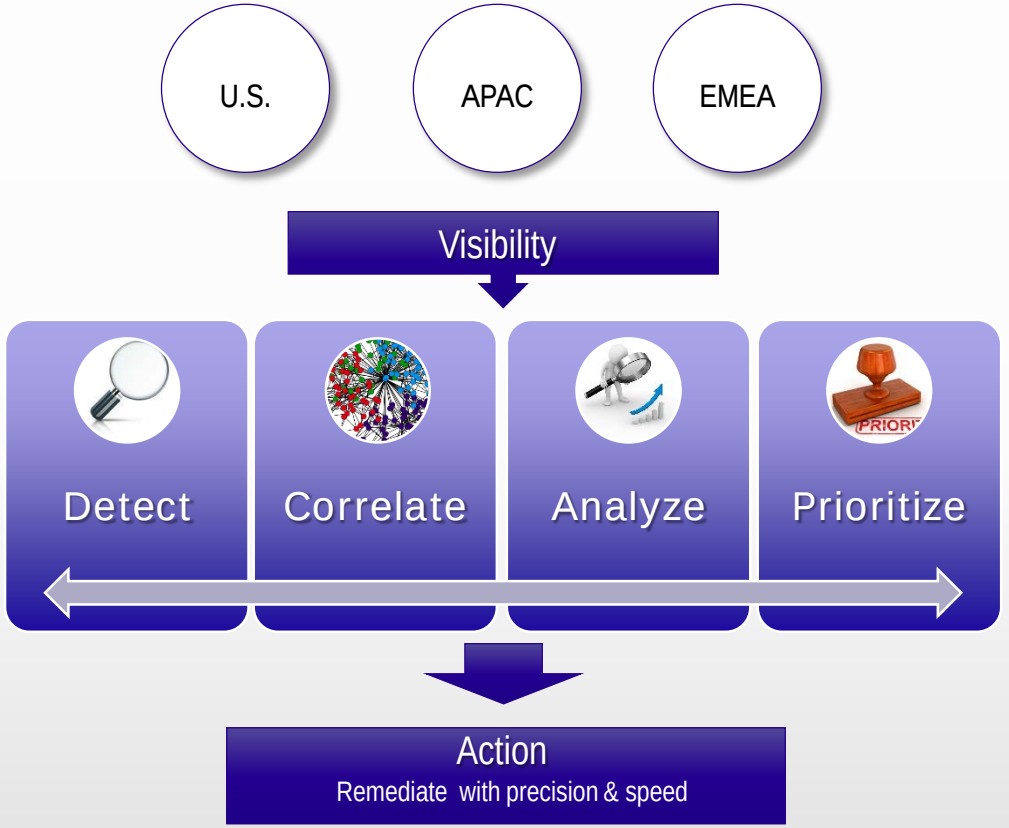
Median # of days before detection

67%

Of victims were notified by external entity

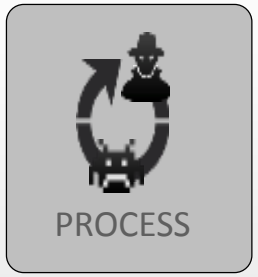
Source: Mandiant M-Trends Report 2012/2013/2014

Cyber Threat Action Center



CTAC Impact

ACTOR



THREAT

- Human directed
- Goal-oriented
- Dynamic (adjusts to changes)
- Coordinated
- Multiple tools & activities
- New evasion techniques

CTAC

- Fusion of people, process, & technology
- Isolated & secure research
- Rapid learning and response
- Sharing & collaboration
- Contextual & behavioral
- Leverage threat intel

IT Info Security Policy Relationship

IT Info Security Policy Relationship

- At a minimum, SOC development should address the requirements of your IT Information Security policy.
- The policy should also aid the SOC by:
  - Monitoring and coverage requirements (24x7 model or off-hours)
  - Mandated training for SOC teams on a regular (min. annual) basis
  - Incident Response intake, escalation and reporting requirements
  - Data classification standard (HIPAA, ePHI/PHI, PII, PCI)

CTAC Structure

The Right People

- Initial CTAC Team Consists of:
  - 4 Level I Analysts (1-2 years of fundamentals)
  - 3 Level II Analysts (3-5 years of full-spectrum experience)
  - 2 Level III Analysts (dedicated researchers)
- Supported by:
  - 4 SIEM Engineers
  - 3 Vulnerability Management Analysts
  - 3 Device/Tool Admins

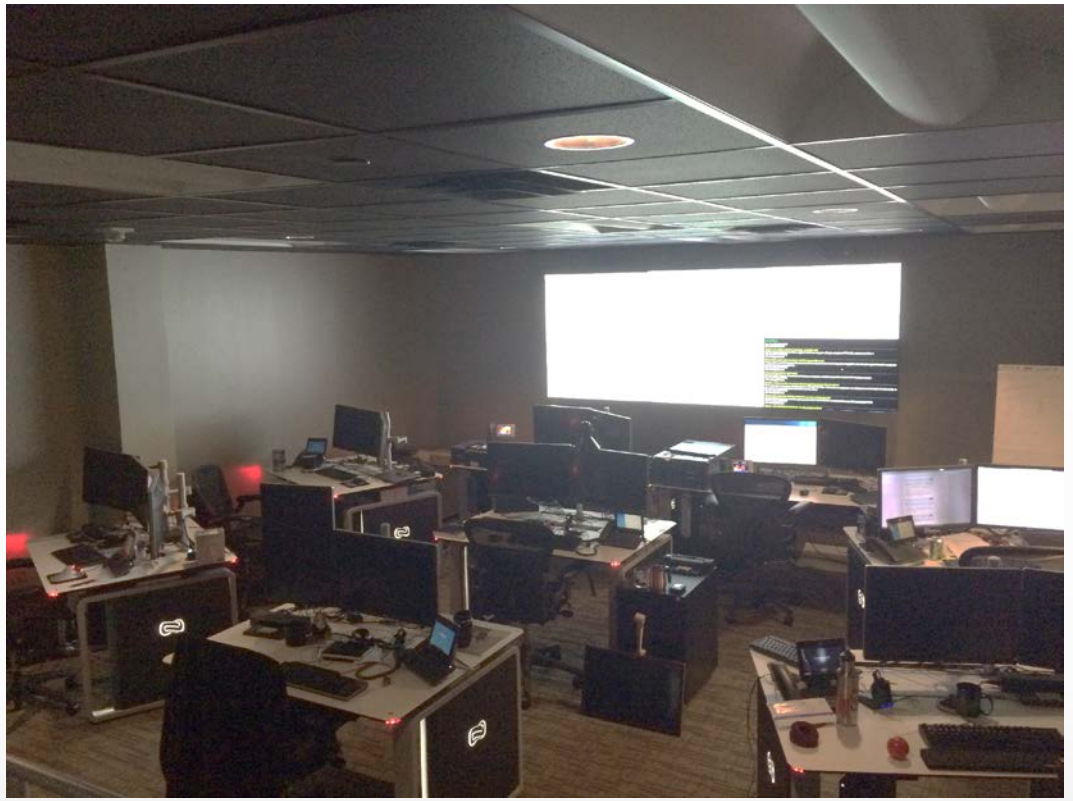
The Right Processes and Technology

- Implement security controls
  - Archer GRC aids IT Compliance
- Increase visibility of Enterprise network events
  - SIEM indexes big data and makes it searchable
- Correlate findings and establish context
  - Off-the-shelf and custom in-house-developed applications
- Automate event/incident response
  - Archer Security Operations

Security best-practice Insecure activity Emerging compliance issues

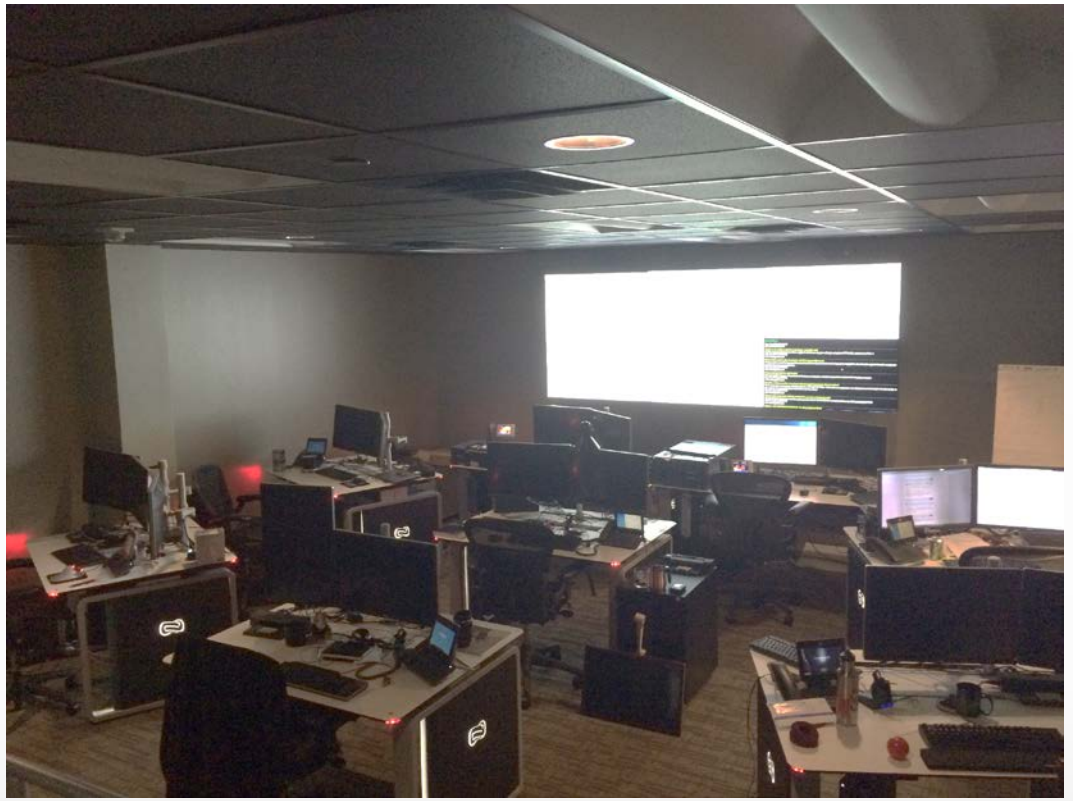
Physical Build-Out

- Fully-configurable video wall
- 6 mechanical sit-stand desks
- 2 fixed full-size desks
- 1 hoteling position
- Forensic area
- Vulnerability Mgmt area
- Intel Operations area
- Secure conference room w/ VTC
- Senior office
- Server room



Physical Build-Out

- All HVAC and facility boundaries are built to eliminate any ability to eavesdrop or overhear activities.
- Double-paned, tempered glass used for our observation window from the public hallway.
- Include a window shade for use during sensitive functions.



SOC Must Foster Secure Collaboration

Need-to-know basis starts in a contained, regulated process

Don’t allow the unfounded to become externally unproductive:

- Events can become incidents. A SOC must contain this narrative.
- Discussion frequently needs to be rapid and open. Secure it.
- Sensitive personnel issues are common. The venue must respect this.

The Unexpected

The Unexpected

- Cosmetic considerations count. We have an external display w/ security awareness slides outside.
- Anticipate physical expansion in your blueprint. It may happen – soon. Keep things re-configurable where possible.
- Fundamental operations come first. Keep analyst downtime low during construction and transition.
- Keep your pre-SOC processes alive for DR/BC. Redundancy is key. Update them accordingly.

The Unexpected

A new SOC changes many things, some counter-intuitively

- Dispel sociopolitical issues of ‘isolationism’ early. Invite reasonable visitation and have an open house.
- Avoid creating a message that defense is absolute because the SOC has arrived.
- Market the SOC as member of the IT business.
- Get a logo, get swag to hand out: mouse pads, stickers

The Unexpected

- ADA requirements will affect your physical layout and can come as a surprise. Plan for these *early.*
- This door opened into a high-traffic hallway because of access ramp inside.
- Many costly solutions proposed ($10-50k)

The Unexpected

- Be creative where permissible.

Questions?

Thank you!